Geräte per Web-Browser aus der Ferne steuern und überwachen

Eine neue Technologie von Applied Informatics ermöglicht den unkomplizierten und sicheren Fernzugriff auf den Web-Server eines Embedded Systems, selbst wenn sich das Gerät hinter einem NAT Router oder einer Firewall befindet und keine öffentliche IP Adresse hat.

Bei Netzwerk-basierten Embedded-Systemen sind web-basierte Benutzerschnittstellen mittlerweile Standard. Mit ihnen werden über PC, Smart Phone oder iPad Geräte über einen Web-Browser konfiguriert, bedient und überwacht. Dank leistungsfähiger Web-Browser, JavaScript und Ajax Programmiertechniken sind web-basierte Benutzerschnittstellen sehr leistungsfähig und benutzerfreundlich. Da sie lediglich eine HTTP(S) Verbindung zwischen Web-Browser und dem auf dem Gerät laufenden Server benötigen, sind sie sehr gut aus der Ferne nutzbar. Voraussetzung ist jedoch, dass der Web-Browser eine HTTP Verbindung zum Server im Gerät aufbauen kann. Das funktioniert nur, wenn sich das Gerät im selben Netzwerk wie der Web-Browser befindet oder das Gerät direkt mit dem Internet verbunden und über eine öffentliche IP Adresse erreichbar ist. Leider sind diese Voraussetzungen in der Praxis kaum gegeben. Häufig befinden sich Geräte in privaten Netzen hinter NAT Routern oder Firewalls. Selbst für Geräte, die sich in einem mobilen Netz wie GSM/GPRS oder UMTS befinden, werden oft nur private IP-Adressen vergeben. Damit ist es zwar für das Gerät möglich das Internet zu erreichen; umgekehrt kann aber das Gerät nicht direkt über das Internet angesprochen werden.

INTERNET-BASIERTER FERNZUGRIFF AUF GERÄTE MIT REVERSE HTTP

Port Forwarding und Virtual Private Network (VPN) sind bekannte technische Möglichkeiten des Internet-basierten Fernzugriffs auf Geräte. Doch beide Varianten sind für den Einsatz von Embedded Systemen nicht ideal und sehr aufwändig. Daher hat Applied Informatics eine neue Technologie entwickelt, die eine echte Alternative zu Port Fowarding und VPN ist. Mit Reverse HTTP kann man schnell, sicher und unkompliziert auf den Web-Server eines Gerätes zugreifen – auch aus der Ferne. Wie dies funktioniert und wofür diese Technologie genutzt werden kann wird nachfolgend erklärt.

TECHNOLOGIE MIT TRICK: REVERSE HTTP

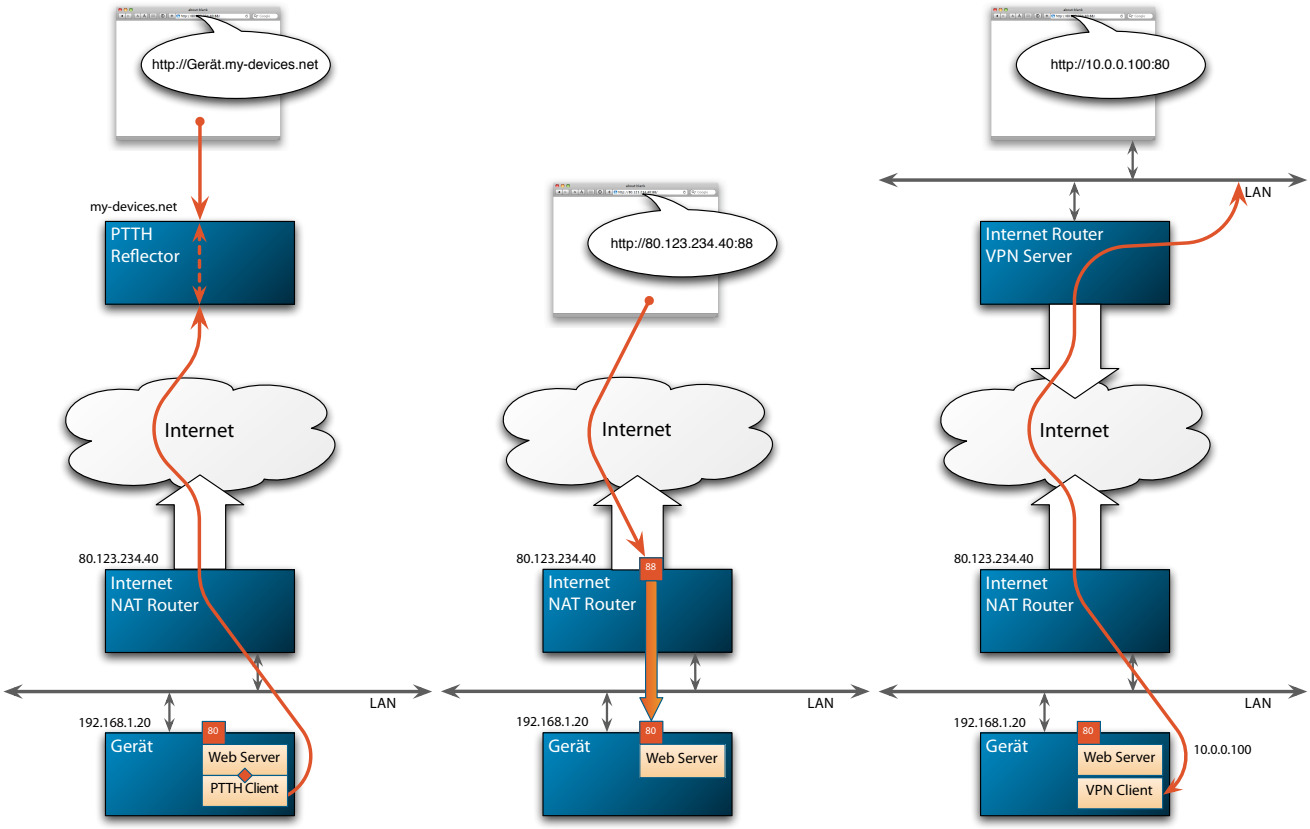
Bei Reverse HTTP (PTTH) handelt es sich um eine recht einfache Abwandlung des HTTP Protokolls. Der wesentliche Unterschied zu HTTP besteht darin, dass das Gerät mit dem Web-Server von sich aus eine Verbindung zu einem speziellen Server, dem so genannten Reverse HTTP Reflector, aufbaut. Das ist so gut wie immer möglich, egal über welche Technologie das Gerät Zugriff auf das Internet hat – sogar über einen HTTP Proxy Server. Der Trick besteht nun darin, dass die Verbindung sozusagen umgedreht wird, sobald sie aufgebaut ist. Der Reverse HTTP Reflector kann über die nun bestehende Verbindung Anfragen zum Gerät senden, die dann vom Web-Server des Gerätes beantwortet werden. Der Reverse HTTP Reflector enthält ebenfalls einen Web-Server, welcher Anfragen vom Web-Browser des Benutzers entgegennimmt, und diese Anfragen dann über die Reverse HTTP Verbindung des Gerätes an den Web-Server des Gerätes transparent weiterleitet.

Einsatzmöglichkeiten

- Fernzugriff auf Datenlogger, z. B. im Bereich erneuerbare Energien (Photovoltaik- und Windkraftanlagen), Umwelttechnik (Messstationen), Verkehrstechnik.
- Smart Metering (Fernzugriff auf intelligente Stromzähler oder Smart Metering Gateways)
- Zugriff auf mobile Geräte, z. B. im Bereich mobile Datenerfassung, Tracking, Fleet Management, usw.
- Fernwartung von Geräten der Konsumelektronik und Haustechnik (z. B. im Bereich Heimvernetzung, Set-Top Boxen, Heizungs- und Klimatechnik, usw.)
- Fernwartung von Maschinen und Anlagen, sowie im Bereich Gebäudeautomatisierung
- Fernzugriff auf Ticketing- und Zutrittskontrollsysteme

TIPPS FÜR DEN BETRIEB

Der Reflector muss natürlich wissen, an welches Gerät die Anfrage weiterzuleiten ist. Dies kann entweder über die Web Adresse (URL) erfolgen (z. B. *http://MeinGerät.my-devices.net*) oder über einen Cookie, der nach erfolgtem Login-Vorgang am Reflector Server im Browser des Clients gesetzt wird. Bei ersterer Methode wird im DNS Server ein Wildcard Eintrag definiert welcher alle Zugriffe auf **.my-devices.net* auf den Reflector Server *www.my-devices.net* weiterle-



Reverse HTTP (links), NAT Port Forwarding (mitte) und VPN (rechts) im Vergleich

itet. Der Server kann dann anhand des Host Headers im HTTP Request, sowie einer Zuordnungstabelle erkennen, welches Gerät gemeint ist, und die Anfrage entsprechend weiterleiten. Der für dieses Verfahren notwendige Reverse HTTP Reflector Server kann entweder selbst betrieben werden oder es wird ein von einem Dienstleister betriebener Server benutzt. Für den Betrieb des Reflector Servers eignen sich sehr gut Cloud Services, wie sie von Amazon (EC2) oder Rackspace angeboten werden.

UNBEDENKLICHER EINSATZ: DATENSICHERHEIT IST GEGEBEN

Da der Reflector Server selbst keinerlei Daten speichert, sondern die HTTP Anfragen nur transparent weiterleitet, ist diese Methode auch aus dem Betrachtungswinkel der Datensicherheit weitestgehend unbedenklich. Selbstverständlich kann sowohl die Reverse HTTP Verbindung vom Gerät zum Reflektor, als auch die HTTP Verbindung vom Browser zum Reflector mit SSL, bzw. TLS verschlüsselt werden. Ein einzelner unter Linux laufender Reflector Server kann leicht mehrere tausend Geräte bedienen, mit bis zu 100 oder mehr simultanen Browser-Zugriffen. Ein großer Vorteil dieser Methode ist, dass sie eine sehr sichere Anbindung der Geräte ermöglicht. Da das Gerät nur über die zum Reflector Server aufgebaute Verbindung und somit nur über den Reflector Server erreichbar ist, besteht keine Gefahr durch Denial-of-Service Angriffe auf das Gerät. Zugriffe auf das Gerät über den Reflector erfordern natürlich eine vorhergehende Authentifizierung des Benutzers. Auch das Gerät selbst muss sich gegenüber dem Reflector Server authentifizieren. Dies kann entweder über ein Passwort erfolgen oder über ein digitales Zertifikat. Nachteil des Verfahrens ist, dass nur HTTP Zugriff auf das Gerät möglich ist, nicht aber FTP oder ein Shell-Login.

AUCH WEB SERVICES MÖGLICH

Reverse HTTP kann natürlich nicht nur dazu benutzt werden, um auf Web Seiten auf dem Gerät zuzugreifen. Jeder auf HTTP basierende Kommunikationsmechanismus kann auch über Reverse HTTP verwendet werden, so z. B. auch Web Services, welche auf SOAP, JSON oder REST Technologie basieren.

UMSTIEG LEICHT GEMACHT

Die für die Integration von Reverse HTTP in ein Gerät notwendige Software sowie der Reflector Server werden von Applied Informatics angeboten. Bestehende Geräte, bei denen eine entsprechende Erweiterung der Software nicht möglich ist, können über ein spezielles Gateway-Device angebunden werden. Das Gateway befindet sich im selben Netz wie das Gerät, verbindet sich mit dem Reflector Server, und leitet die Anfragen vom Reflector Server an das jeweilige Gerät weiter.

Reverse HTTP in Verbindung mit einem Reflector Server stellt eine hervorragende Alternative zu Technologien wie VPN und NAT Port Forwarding dar, um das Web Interface eines Gerätes per Fernzugriff nutzbar zu machen. Diese neue Technologie lässt sich ohne Eingriff in die Netzwerk Infrastruktur einsetzen; der notwendige Reflector Server kann auch „in der Cloud", oder durch einen Dienstleister betrieben werden. Auf Geräteseite ist entweder die Integration einer Reverse HTTP Client Software erforderlich, was ohne großen Aufwand möglich ist, oder die Anbindung erfolgt über einen speziellen Gateway.

LIVE DEMONSTRATION

Eine Demonstration der Reverse HTTP Technologie von Applied Informatics steht unter http://my-devices.net zur Verfügung. Die für die Demonstration erforderliche Zugangskennung mit Passwort kann über die Seite http://www.appinf.com/de/company/contact.html angefordert werden.

Technologien	Vorteile	Nachteile
Reverse HTTP	> einfache Abwandlung des bewährten HTTP Protokolls > Technologie lässt sich ohne Eingriff in die Netz-Infrastruktur einsetzen > sichere, verschlüsselte Verbindungen möglich > der notwendige Reflector Server kann auch in der Cloud laufen > Anbindung bestehender Geräte über spezielles Gateway möglich > hohe Skalierbarkeit, bis zu tausenden von Geräten	> spezieller Reflector Server muss betrieben werden, wobei dies auch durch einen spezialisierten Dienstleister erfolgen kann > auf Geräteseite ist entweder ist die Integration einer Reserve HTTP Client Software erforderlich, oder ein Gateway wird verwendet > nur Zugriff über HTTP möglich
Port Forwarding	> prinzipiell einfache Möglichkeit > per HTTP wird auf ein Gerät hinter einem NAT Router zugegriffen > Problem mit der IP-Adresse kann mit Diensten wie Dynamic DNS in den Griff bekommen werden	> muss am NAT Router aktiviert werden; umständlich (bei mehreren Geräten braucht jedes Gerät eine eigene öffentliche Portnummer) > NAT Router haben üblicherweise keine fixen IP-Adressen > durch direkte Anbindung ans Internet ist Gerät ein leichtes Ziel für Denial-of-Service Angriffe; Systeme können so schnell und leicht unbrauchbar gemacht werden
Virtual Private Network	> es wird ein sicherer Tunnel durch das Internet errichtet, über das ein Gerät direkt in ein anderes Netzwerk wie ein Unternehmens-LAN integriert wird > verschlüsselte, sichere Verbindung	> nicht alle Internet-Provider ermöglichen VPN > Aufbau der notwendigen Netzwerk-Infrastruktur ist sehr aufwändig, vor allem wenn viele Geräte integriert werden müssen

KONTAKT

Applied Informatics Software Engineering GmbH
St. Peter 33
9184 St. Jakob im Rosental
Austria

T +43 4253 32596 **F** +43 4253 32096
info@appinf.com | www.appinf.com

applied informatics